

§ 164.102

164.318 Compliance dates for the initial implementation of the security standards.

APPENDIX A TO SUBPART C—SECURITY STANDARDS: MATRIX

Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information

- 164.400 Applicability.
- 164.402 Definitions.
- 164.404 Notification to individuals.
- 164.406 Notification to the media.
- 164.408 Notification to the Secretary.
- 164.410 Notification by a business associate.
- 164.412 Law enforcement delay.
- 164.414 Administrative requirements and burden of proof.

Subpart E—Privacy of Individually Identifiable Health Information

- 164.500 Applicability.
- 164.501 Definitions.
- 164.502 Uses and disclosures of protected health information: General rules.
- 164.504 Uses and disclosures: Organizational requirements.
- 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.
- 164.508 Uses and disclosures for which an authorization is required.
- 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.
- 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.
- 164.514 Other requirements relating to uses and disclosures of protected health information.
- 164.520 Notice of privacy practices for protected health information.
- 164.522 Rights to request privacy protection for protected health information.
- 164.524 Access of individuals to protected health information.
- 164.526 Amendment of protected health information.
- 164.528 Accounting of disclosures of protected health information.
- 164.530 Administrative requirements.
- 164.532 Transition provisions.
- 164.534 Compliance dates for initial implementation of the privacy standards.

AUTHORITY: 42 U.S.C. 1320d-1320d-8; sec. 264, Public Law 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320-2 (note)); secs. 13400 and 13402, Public Law 111-5, 123 Stat. 258-263.

SOURCE: 65 FR 82802, Dec. 28, 2000, unless otherwise noted.

45 CFR Subtitle A (10-1-10 Edition)

Subpart A—General Provisions

§ 164.102 Statutory basis.

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act, section 264 of Public Law 104-191, and section 13402 of Public Law 111-5.

[74 FR 42767, Aug. 24, 2009]

§ 164.103 Definitions.

As used in this part, the following terms have the following meanings:

Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with § 164.105(a)(2)(iii)(C).

Hybrid entity means a single legal entity:

- (1) That is a covered entity;
- (2) Whose business activities include both covered and non-covered functions; and

- (3) That designates health care components in accordance with paragraph § 164.105(a)(2)(iii)(C).

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

- (1) Investigate or conduct an official inquiry into a potential violation of law; or
- (2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Plan sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

Required by law means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

[68 FR 8374, Feb. 20, 2003, as amended at 74 FR 42767, Aug. 24, 2009]

§ 164.104 Applicability.

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this part apply to the following entities:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, or other than as a business associate of a covered entity, the clearinghouse must comply with § 164.105 relating to organizational requirements for covered entities, including the designation of health care components of a covered entity.

[68 FR 8375, Feb. 20, 2003]

§ 164.105 Organizational requirements.

(a)(1) *Standard: Health care component.* If a covered entity is a hybrid entity, the requirements of subparts C and E of this part, other than the requirements of this section, § 164.314, and § 164.504, apply only to the health care component(s) of the entity, as specified in this section.

(2) Implementation specifications:

(i) *Application of other provisions.* In applying a provision of subparts C and E of this part, other than the requirements of this section, § 164.314, and § 164.504, to a hybrid entity:

(A) A reference in such provision to a “covered entity” refers to a health care component of the covered entity;

(B) A reference in such provision to a “health plan,” “covered health care provider,” or “health care clearinghouse,” refers to a health care component of the covered entity if such health care component performs the functions of a health plan, health care provider, or health care clearinghouse, as applicable;

(C) A reference in such provision to “protected health information” refers to protected health information that is created or received by or on behalf of the health care component of the covered entity; and

(D) A reference in such provision to “electronic protected health information” refers to electronic protected health information that is created, received, maintained, or transmitted by or on behalf of the health care component of the covered entity.

(ii) *Safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this section and subparts C and E of this part. In particular, and without limiting this requirement, such covered entity must ensure that:

(A) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which subpart E of this part would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care component and the other component were separate and distinct legal entities;